

ORIGINAL

RECEIVED

SEP 29 2000

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

TELECOMMUNICATIONS®
TIA
INDUSTRY ASSOCIATION

September 29, 2000

The Honorable William E. Kennard
Chairman
Federal Communications Commission
445 12th Street, S.W.,
Washington, DC 20554

EX PARTE OR LATE FILED

**Re: In the Matter of Communications Assistance for Law
Enforcement Act, CC Docket No. 97-213**

Dear Chairman Kennard:

The Telecommunications Industry Association ("TIA") respectfully submits the attached *Report on Surveillance of Packet-Mode Technologies* for the Commission's consideration.

In its *Third Report and Order*,¹ the Commission considered the issue of CALEA compliance for packet-mode communications. Although the Commission expressed some concerns with the technical solutions provided by the industry safe harbor standard (J-STD-025),² it decided that CALEA solutions consistent with J-STD-025 should be provided by September 30, 2001.

At the same time, however, the Commission noted "that packet-mode technology is rapidly changing, and that different technologies may require differing CALEA solutions." The Commission also recognized that "we must avoid implementing CALEA requirements that could impede the development of new technologies" and concluded that "[w]e do not believe that the record sufficiently addresses packet technologies and the problems that they may present for CALEA purposes." As a result, the Commission requested that TIA further study the technical issues concerning the surveillance of packet mode technologies and submit a report to the Commission by September 30, 2000.

¹ In the Matter of Communications Assistance for Law Enforcement Act, *Third Report and Order*, CC Docket No. 97-213, FCC 99-230, ¶ 55 (rel. August 31, 1999) ("Third Report & Order").

² Telecommunications Industry Association & Alliance for Telecommunications Industry Solutions, Interim Standard, *Lawfully Authorized Electronic Surveillance*, J-STD-025 (December 1997).

No. of Copies rec'd 041
List ABCDE

As mentioned in TIA's previous status reports to the Commission,³ TIA immediately formed a working group, drawing on the technical expertise of its various standards committees, to provide technical input to this study. In order to expand the technical expertise contributing to the packet data study, TIA also invited a broad variety of packet-oriented technical groups to participate in a series of Joint Experts Meetings ("JEM"). The first session of the JEM was held on May 3-5, 2000 in Las Vegas, Nevada. The second session was held in Washington, D.C. from June 27-29.

TIA appreciates the hard work and contributions made by all of the companies and organizations that participated in the JEM process. Both sessions of the JEM were well attended and sparked lively discussion. Participants included not only a broad spectrum of the industry, but also representatives from the Federal Bureau of Investigation and the Center for Democracy and Technology. TIA was especially pleased that representatives of the Commission's staff were able to participate in both meetings. A list of attendees from the two sessions is attached.

Without attempting to summarize the entire *Report*, TIA would like to draw the Commission's attention to a few, critical issues raised during the Joint Experts Meetings.

- **Packet-Mode Services Are Extremely Varied and Diverse.** As the Commission properly noted in its *Third Report and Order*, "packet technologies are rapidly changing and different technologies may require differing CALEA solutions for separating call-identifying information from call content." The JEM's experience fully validates the Commission's statement. Although a large group of experts in a wide variety of different packet data technologies participated in the discussions, the JEM was able to evaluate only a fraction of the technologies currently being used or developed. The JEM also noted that packet data protocols vary significantly and that any one packet data standard is unlikely to work for all protocols – unless some "one-size-fits-all" approach (such as that identified in J-STD-025) is adopted. As a result, it may be appropriate for the Commission to encourage separate standards for each, individual packet technology (for example, PacketCable's standard for packetized cable telephony).
- **The Uncertain Legal Framework Complicates Development Efforts.** TIA viewed its mandate from the Commission to be fairly narrow – to discuss the technical issues raised by the Commission and not to address legal questions such as what constitutes "call-identifying information" for a packet-mode service or whether a particular packet-mode technology is a "communications service" or "information service" for purposes of CALEA. TIA considered those questions to be outside of the scope of the Commission's

³ Telecommunications Industry Association, *Status Report*, CC Docket No. 97-213 (filed on December 23, 1999); Telecommunications Industry Association, *Second Status Report*, CC Docket No. 97-213 (filed on May 17, 1999).

request. Nevertheless, the JEM discussion repeatedly demonstrated that technical analysis of what was feasible or infeasible depended on such legal issues. The JEM participants were frequently frustrated by the fact that there was no clear, legal framework (either in the statute or from the Commission's decisions) in which to base their evaluations. For example, it is ambiguous how the term "call-identifying information" applies (if at all) to packet data. Without clearer guidance of what constitutes "call-identifying information" for packet data, industry cannot accurately report on the technical impact and feasibility of making such information available to law enforcement. Similarly, just because a specific packet mode technology is discussed in the *Report* does not mean that the JEM viewed the technology as being a communications services for purposes of CALEA.

- **Technical Difficulty of Analyzing Packet Data Traffic.** Because of the inherent flexibility of packet-mode technologies, these technologies are used to transport a theoretically unlimited number of different services, applications and protocols. New protocols are being introduced almost daily. It is not technically feasible to determine, on a packet by packet basis, the application or service that is being provided in a particular packet stream. Encapsulation (i.e., wrapping packets within packets) and encryption of packets renders identification of the type of service being conveyed (e.g., communication vs. information) even more difficult, if not possible. As a result, it would be a significant burden to try to analyze packets in a real-time basis to extract the kind of information that law enforcement might wish to obtain. (For example, the information could be buried within several layers of encapsulated packets, within a protocol with which the carrier transporting the packet has no familiarity).
- **Call-Management Servers vs. Sessions Without Call-Management Servers.** This identification and analysis problem may be less severe with technologies that have call set-up and tear-down capabilities – i.e., technologies that include a Call Management Server ("CMS"). As the JEM noted, the point where a CMS sets up a communication may be the only time that a packet-mode communication service can be distinguished from an information service and that call-identification-like information might be identified. Again, however, what might be feasible will vary widely from CMS-technology to CMS-technology. For transport services without a CMS, it is extremely burdensome to segregate individual packets out of the stream of packets being conveyed by the transport carrier and extract the kind of information law enforcement is requesting. In those transport technologies, where the whole packet stream must be examined in order to gather relevant call-identification-like information, the process of filtering may overload the network's processing capacity or severely degrade network performance.
- **FBI's Carnivore Presentation.** During the JEM's second session, the FBI gave a presentation on its existing packet-data surveillance device (nicknamed "Carnivore"). The "Carnivore" presentation from the FBI was extremely enlightening. First, it verified the "gut feel" of the JEM's technical experts that development of a filter protocol like

Carnivore is extremely resource intensive and fluid because of the ever changing nature of packet protocols and the constant introduction of new protocols. As the FBI acknowledged, requiring carriers and equipment vendors to develop similar filtering technology would be extremely expensive and burdensome. Second, at least as explained by the FBI, the Carnivore device would allow law enforcement to conduct the kind of filtering envisioned by J-STD-025, thus raising the question whether it would be cost-effective (or even privacy-protective) to require carriers to develop their own, separate capabilities.

- **Most Cost-Efficient and Technically-Feasible Solution.** The consensus among the JEM participants was that (for the reasons discussed above and in more detail in the *Report*) providing the entire packet stream for a particular subscriber is by far the most cost-effective and technically feasible method for providing access to law enforcement. Of course, in order to address privacy concerns, law enforcement must obtain the appropriate legal authorization to receive this packet stream (such as a Title III order) and strict legal procedures should be adopted to assure compliance with the limits on that authorization. To require carriers to develop a filtering program would be extremely burdensome and expensive (requiring continuous updates and modifications) – especially for non-CMS packet services. For some CMS services, it might be possible to separate call-identification-like information from content – but what would be feasible will vary from technology to technology and would require individual standards.

In conclusion, TIA would encourage the Commission to establish a procedure by which CALEA solutions for packet data technologies could be implemented in a more efficient and rational method. As TIA noted in its recent comments in this docket,⁴ the Commission should immediately suspend the September 30, 2001 compliance deadline pending the completion of any proceedings the Commission may initiate after evaluating this *Report*. Manufacturers and carriers are unsure whether to continue expending considerable resources developing complicated and expensive solutions consistent with the J-STD-025, if it is possible that those solutions may prove to be only an “interim” or “temporary remedy.” By suspending the deadline, the Commission will enable itself to solicit comments on the *Report* and make a final, informed decision.

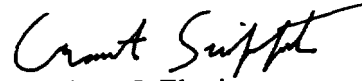
TIA appreciates the confidence expressed by the Commission in entrusting to TIA the responsibility for preparing this *Report*. If you have any questions about the *Report*, please do not hesitate to contact me.

⁴ Telecommunications Industry Association, *Comments*, CC Docket No. 97-213 (filed September 15, 2000).

The Honorable William E. Kennard
September 29, 2000
Page 5

Pursuant to 47 C.F.R. § 1.1206, copies of the *Report* will be filed with the Commission's Secretary. TIA is also providing copies of this *Report* to several of the Commission staff involved in this proceeding.

Sincerely,



Matthew J. Flanigan

President

Grant Seiffert

Vice President, Government Relations

cc (w/encl.): The Honorable Harold Furchtgott-Roth
The Honorable Susan Ness
The Honorable Michael Powell
The Honorable Gloria Tristani

CALEA JEM Attendance Roster

* : attended JEM II but not JEM I
 - : attended JEM I and JEM II
 : attended JEM I but not JEM II

-Ahmed Patel	Worldcom	ahmed.patel@wcom.com
-Al Gidari	G-savvy.com	gidari@worldnet.att.net
*Al Thomas	BellSouth Cellular	al_thomas@bscc.bcs.com
*Art Stefanelli	Raytheon	astefanelli@fallschurch.esys.com
-Ben Ederington	Steptoe & Johnson, LLP	bederington@steptoe.com
Ben Leviton	GTE	Bleviton@tsi.gte.com
Bernd Adams	Deutsche Telekom AG	Bernd.adams@telekom.de
Bernhard Spalt	Siemens AG	Bernhard.spalt@siemens.it
Bernie McKibben	Motorola	p17982@email.mot.com
-Bill Krehl	Siemens	Bill.krehl@icn.siemens.com
-Bill Marshall	AT&T Wireless	wtm@research.att.com
-Bob Hall	SBC	bhall@trc.sbc.com
Bob Marks	Lucent	rjmarks@lucent.com
Bora Biray	Siemens ICN	bora.biray@icn.siemens.com
-Brye Bonner	Motorola	brye.bonner@motorola.com
-Cathy Fitzpatrick	Lucent	fitz50@lucent.com
Charlie Ross	Verizon Wireless	ross1ch@bam.com
Cheryl Blum	Lucent	cjblum@lucent.com
-Chip Sharp	Cisco Systems	chsharp@cisco.com
Chuck Gerlarch	Lucent	gerlachc@lucent.com
Chuck Ishman	Motorola	gaoo6@email.mot.com
-Dan Yong	Bell Atlantic	danny.yong@bellatlantic.com
:Dave Thompson	TIA	dthompso@tia.eia.org
David Cushman	Motorola	cushman@cig.mot.com
David Hoffman	US West Interprises	dwhoffm@uswest.com
David Rich	Worldcom	dave.rich@wcom.com
*David Ward	FCC	doward@fcc.gov
-Dean Anderson	Lucent	dba@lucent.com
-Derek Khlopin	TIA	dkhlopin@tia.eia.org
DeWayne Sennett	AT&T Wireless	dewayne.sennett@attws.com
*Dick Nichols	Icon-O-Voice	dnichols@iconovoice.com
Don Auble	SBC	donald.e.auble@ameritech.com
-Don Bender	USTA	dbender@usta.org
Ed Campbell	3Com Corporation	ed_campbell@3com.com
Ed Chan	Verizon Wireless	chaned@bam.com
Ed Hall	CTIA	ehall@ctia.org
Edward O'Leary	Rogers Wireless	eoleary@rci.rogers.com
Fabio Maino	Cisco Systems	Fmaino@cisco.com
-Gary Pellegrino	Verizon Wireless	gpellegr@mobile.bam.com
Jack Nasielski	Qualcomm	jackn@qualcomm.com
-James Polk	Cisco Systems	jmpolk@cisco.com
-Jay Hilton	Telcordia (T1)	jhilton@telcordia.com
Jean Bouin	Alcatel	jean.bouin@space.alcatel.fr
-Jerry Stanshine	FCC	jstanshi@fcc.gov
-John Barna	Ericsson	john.barna@ericsson.com
-John Menard	Lucent	imenard@lucent.com
*John Piker	CIS-FBI	???
John Richardson	Intel	jwr@intel.com

* John Yu	Booz, Allen & Hamilton	???
Kathleen Garrett	Nortel Networks	kgarrett@nortelnetworks.com
Keith Bromley	Ericsson	keith.bromley@ericsson.com
-Ken Coon	Telcordia	kcoon@telcordia.com
Kimberly King	AT&T Wireless	kimberly.king@attws.com
Leu L. Wu	Lucent	leuwu@lucent.com
-Lou Degni	CALEA CIS	
-Marion Finck	Siemens ICN	marion.finck@icn.siemens.com
*Mark Montz	Compaq	mark.montz@compaq.com
-Mark Munson	GTE	mmunson@mobilnet.gte.com
*Mark Younge	Voicestream Wireless	mark.Younge@voicestream.com
Michael Francis	CALEA	francism@erols.com
-Michael Gallagher	CALEA	
*Montgomery Kosma	Gibson, Dunn & Crutcher LLP / CTIA	mkosma@gdclaw.com
-Peter Musgrove	AT&T Wireless	peter.musgrove@attws.com
-Pete Streng	Nortel Networks	streng@nortelnetworks.com
-Pierre Truong	Ericsson	pierre.truong@ericsson.com
*Richard Dodd	Davis, Wright & Tremaine	rickdodd@dwt.com
Ron Ryan	Nortel (T1P1)	Rryan@nortelnetworks.com
*R. Arifin	Hughes Network Systems	rarifin@hns.com
*Scott Yagel	Alcatel	syagel@usa.alcatel.com
*Sean Kim	Booz-Allen & Hamilton	(703) 289-5220
Serge Caron	Nortel Networks	Scaron@nortelnetworks.com
-Sherry Hsieh	Tachion Networks	Sherrih@tachion.com
*Steve Titcombe	GlobalStar	steve.titcombe@gobalstar.com
-Terri Brooks	Nokia	terri.brooks@nokia.com
-Terry Watts	SBC Technology	twatts@tri.sbc.com
Theroen Dorenbosch	Motorola	fjd007@email.mot.com
-Thomas Richter	BellSouth Cellular	thomas_richter@bscc.bs.com
*Todd Lanter ???	PCIA	lantert@pcia.com
-Warren Sims	Ericsson	warren.sims@ericsson.com
Wayne Bowen	USPhoenix/CDT	usphoenix@aol.com
Wayne Zeuch	Lucent (T1)	zeuch@lucent.com
-William Waung	Lucent	wwaung@direct.ca

Report to the
Federal Communications Commission
on Surveillance of
Packet-Mode Technologies

(September 29, 2000)

**Prepared by the Joint Experts Meeting convened by Committee TR
45 of the Telecommunications Industry Association**

Report on Surveillance of Packet-Mode Technologies

	Table of Contents	1
1	Introduction.....	2
1.1	Purpose and Scope	2
1.2	Organization.....	2
2	References.....	3
3	Acronyms.....	6
4	Introduction and Executive Summary	9
4.1	Convening the JEM.....	9
4.2	JEM I Output.....	10
4.3	JEM II Output	11
5	Packet Communication Sessions established by a Call Management Server.....	14
5.1	Information that can be reported	14
5.2	Technical Impacts	14
6	Packet Communication Sessions established without a Call Management Server...	15
6.1	Information that can be reported, subject to technical impact analysis	15
6.2	Technical Impacts	15
6.2.1	Delivering the Entire Packet Stream.....	15
6.2.2	Delivery of Header routing information	16
6.2.3	Extraction of Pen Register or Trap and Trace information.....	16
	Appendix A : Technology Specific Information	18
A.1	Access Networks.....	18
A.1.2	CDMA2000.....	20
A.1.3	GPRS.....	25
A.1.4	CDPD.....	29
A.1.5	Packet Cable.....	33
A.2	Network Layer Protocols.....	41
A.2.1	X.25 Over ISDN Basic Rate Interface.....	41
A.2.2	ATM.....	44
A.2.3	IP.....	45
A.2.4	Frame Relay.....	63
	Appendix B: CALEA JEM Invited and/or Participating Groups List	66
	Appendix C: JEM I Meeting Agenda.....	70
	Appendix D: JEM I Meeting Summary	72
	Appendix E: JEM II Meeting Agenda	79
	Appendix F: JEM II Meeting Summary	81

1 Introduction

In 1997, an industry specification, TIA/EIA/J-STD-025 Lawfully Authorized Electronic Surveillance, was published in response to the Communications Assistance for Law Enforcement Act (CALEA) released in 1994. Privacy concerns have been raised against the packet data solution contained in this specification.

Accordingly, in its Third Report and Order regarding implementation of CALEA, the FCC invited TIA to study CALEA solutions for packet-mode technology and report in one year on "steps that can be taken, including particular amendments to J-STD-025, that will better address privacy concerns." To meet the deadline imposed by the FCC, and to build a record based on technical facts, the Telecommunications Industry Association (TIA) has sponsored two Joint Experts Meetings (JEM). This report represents the findings of these meetings.

1.1 Purpose and Scope

The purpose and scope of this report is to assist the Telecommunications Industry Association (TIA) to prepare a mandated report to the Federal Communications Commission (FCC) regarding certain technical and privacy concerns in packet-mode communications associated with lawfully authorized electronic surveillance under the Communications Assistance for Law Enforcement Act.

1.2 Organization

Section 2 "References" is a list of references used in the preparation of this report.

Section 3 "Acronyms" defines those acronyms that are used in this report.

Section 4 "Introduction and Executive Summary" summarizes the reasons for convening the JEM and the output of JEM I and JEM II.

Section 5 "Packet Communication Sessions established by a Call Management Server" discusses Pen Register and Trap and Trace surveillance of packet-mode communication using a Call Management Server (CMS).

Section 6 "Packet Communication Sessions established without a Call Management Server" discusses Pen Register and Trap and Trace surveillance of packet-mode communication where a CMS is not deployed.

Appendix A "Technical Specific Information" is specific to the technologies discussed in the JEM and includes greater details on surveillance capability of cdma2000, GPRS, CDPD, Packet Cable, X.25, IP, ATM, and Frame Relay.

Appendix B "CALEA JEM Invited and/or Participating Groups List".

Appendix C "JEM I Meeting Agenda".

Appendix D "JEM I Meeting Summary".

Appendix E "JEM II Meeting Agenda".

Appendix F "JEM II Meeting Summary".

2 References

References may be made to specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply, or publications without mention of a specific version, in which case the latest version applies.

American National Standards Institute (ANSI):

[ANSI-95] ANSI/TIA/EIA-95, *800-MHz & 1800MHz CDMA*.

Cable Television Laboratory:

[DOCSIS] SP-RFIV1.1-I05-000714, *Data Over Cable Service Interface Specifications, Radio Frequency Interface Specification*, Cable Television Laboratories, Inc., July 14, 2000.

[PKT-PCES] PKT-SP-ESP-I01-991229, *PacketCable Electronic Surveillance Specification*, Cable Television Laboratories, Inc., December 29, 1999.

[PKT-CODEC] PKT-SP-CODEC-I01-991201, *PacketCable Audio/Video Codecs Specification*, Cable Television Laboratories, Inc., December 1, 1999.

[PKT-NCS] PKT-SP-EC-MGCP-I02-991201, *PacketCable Network-Based Call Signaling Protocol Specification*, Cable Television Laboratories, Inc., December 1, 1999.

[PKT-SEC] PKT-SP-SEC-I01-991201, *PacketCable Security Specification*, Cable Television Laboratories, Inc., December 1, 1999.

European Telecommunications Standards Institute (ETSI):

[GPRS-1] TS 101 113. 3G TS 22.060, *Digital Cellular Telecommunications System (Phase 2+) General Packet Radio Service (GPRS), Service Description; Stage 1* (GSM 02.60).

[GPRS-2] 3G TS 23.060, *General Packet Radio Service Description, Stage 2*.

[ETSI-LI] TS 101 509, *Digital Cellular Telecommunications System (Phase 2+); Lawful Interception; Stage 2*. (GSM 3.33).

[3GPP-LI] 3G TS 33.107, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Architecture and Functions*.

[GSM-1] GSM 02.33 V7.1.0 (1999-07); *Digital Cellular Telecommunications System (Phase 2+); Lawful Interception - stage 1*.

[GSM-2] GSM 03.60 V6.2.0 (1998-10); *Digital Cellular Telecommunication System (Phase 2+); General Packet Radio Service (GPRS); Service Description*.

Federal Communications Commission (FCC):

[FCC 99-230] FCC 99-230, CC-Docket No. 97-213, Third Report and Order, released August 31, 1999.

International Standards Organization:

[ISO8802-3] ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*, 1996.

[ISO8348] ISO 8348: *Information processing systems - data communications - network service definition*.

International Telecommunications Union (ITU):

[X.25] ITU-T Recommendation X.25: *Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet-mode and connected to public data networks by dedicated circuit*.

[Q.931] ITU-T Recommendation Q.931, *ISDN User-network Interface Layer 3 Specification for Basic Call Control*.

Internet Engineering Task Force (IETF):

[RFC0768] Postal, J., *User Datagram Protocol*, August, 1980.

[RFC0791] Postal, J., *Internet Protocol*, September, 1981.

[RFC0826] Plummer, D., *Ethernet Address Resolution Protocol*, November, 1982.

[RFC0894] Horning, C., *Standard for the Transmission of IP Datagrams over Ethernet Networks*, April, 1984.

[RFC1889] Schulzrinne, H., S. Casner, R. Frederick, and V. Jacobson, *RTP: A Transport Protocol for Real-Time Applications*, January, 1996.

[RFC1890] Schulzrinne, H., *RTP Profile for Audio and Video Conferences with Minimal Control*, January, 1996.

[RFC2327] Handley, M., and V. Jacobson, *SDP: Session Description Protocol*, April, 1998.

[RFC1958] Carpenter, B., *Architectural Principles of the Internet*, June 1996.

[RFC2775] Carpenter, B., *Internet Transparency*, February 2000.

[RFC2401] Kent, S. and R. Atkinson, *Security Architecture for the Internet Protocol*, November 1998.

[RFC2804] IAB, *IETF Policy on Wiretapping*, May 2000

[RFC2138] Rigney, C. et. al., *Remote Authentication Dial In User Service (RADIUS)*, April 1997.

[RFC1541] Droms, R., *Dynamic Host Configuration Protocol*, October 1993.

- [RFC2139] Rigney, C., *RADIUS Accounting*, April 1997.
- [RFC1332] McGregor, G., *The PPP Internet Protocol Control Protocol (IPCP)*, May 1992.
- [RFC1918] Rekhter, Y., et. al., *Address Allocation for Private Internets*, February, 1996.
- [RFC1631] Egevang, K., et. al., *The IP Network Address Translator (NAT)*, May 1994.
- [RFC2663] Srisuresh, P. and M. Holdrege, *IP Network Address Translator (NAT) Terminology and Considerations*, August 1999.
- [RFC1702] Hanks, S., et. al., *Generic Routing Encapsulation over IPv4 networks*, October, 1994.
- [RFC1853] Simpson, W., *IP in IP Tunneling*, October 1995.
- [RFC2661] Townsley, M., et. al., *Layer Two Tunneling Protocol 'L2TP'*, August 1999.
- [RFC2406] Kent, S. and R. Atkinson, *IP Encapsulating Security Payload (ESP)*, November 1998.
- [RFC2002] Perkins, C., *IP Mobility Support*, October 1996.
- [RFC1661], Simpson, W., *The Point-to-Point Protocol (PPP)*, July 1994.

Telecommunications Industry Association:

- [IS-835] TIA/EIA/IS-835, *Wireless IP Network Standard for cdma2000*,
- [IS-707-A] TIA/EIA/IS-707-A, *Service Options for CDMA, Revision A*,
- [IS-2000-A] TIA/EIA/IS-2000-A. *Spread Spectrum Systems*,
- [J-STD-025] TIA/ATIS, *Lawfully Authorized Electronic Surveillance*, December, 1997.
- [J-STD-025A] TIA/ATIS, *Lawfully Authorized Electronic Surveillance, Revision A*, May, 2000.
- [IS-732] TIA/EIA/IS-732 *Cellular Digital Packet Data*.

Other:

- [SALTZER] Saltzer J.H., D.P.Reed, D.D.Clark, "*End-To-End Arguments in System Design*", ACM TOCS, Vol. 2, Number 4, November 1984, pp. 277-288.

3 Acronyms

AAA:	Authentication, Authorization and Accounting
AALs	ATM Adaptation Layers
AF:	Access Function
APN:	Access Point Name Data
ASN.1	Abstract Syntax Notation One
ATIS:	Alliance for Telecommunication Industry Solutions
ATM:	Asynchronous Transfer Mode
BRI:	Basic Rate Interface (ISDN)
CDMA:	Code Division Multiple Access
CDPD:	Cellular Digital Packet Data
CF:	Collection Function
CLAMN:	Called Line Address Modification Notification
CLNP:	Connectionless Network Protocol
CM:	Connection Management
CMS:	Call Management Server
CMTS:	Cable Mobile Termination System
DF:	Delivery Function
DHCP:	Dynamic Host Configuration Protocol
DLCI:	Data Link Connection Identifier
DNS:	Domain Name System
DOCSIS:	Data Over Cable Service Interface Specification
DS0:	Digital Signal Level 0
DTMF:	Dual Tone Multifrequency signaling
FDDI:	Fiber Distributed Data Interface
FR:	Frame Relay
GPRS:	General Packet Radio Service
HFC:	Hybrid Fiber-Coax
HPPI:	Hybrid Performance Parallel Interface
HTTP:	Hypertext Transfer Protocol
H.248/megaco	Media Gateway Control - IETF Working Group
H.323:	A standard approved by the International Telecommunication Union (ITU) that defines how conferencing data is transmitted across networks
IANA:	Internet Assigned Numbers Authority
IAP:	Intercept Access Point
IETF:	Internet Engineering Task Force
IMEI:	International Mobile Equipment Identifier
IMSI:	International Mobile Station Identifier
IP:	Internet Protocol
IPSEC:	Internet Protocol Security
IPv4:	Internet Protocol Version 4
IPv6:	Internet Protocol Version 6
ISDN:	Integrated Services Digital Network

ISP:	Internet Service Provider
JEM:	Joint Experts Meeting
L2TP:	Layer 2 Tunneling Protocol
LAN:	Local Area Network
LATA:	Local Access Transport Area
LAES:	Lawfully Authorized Electronic Surveillance
M-ES:	Mobile End System
MAC:	Medium Access Control
MD-IS:	Mobile Data Intermediate System
MDBS:	Mobile Data Base Station
MG:	Media Gateway
MGC:	Media Gateway Controller
MGCP:	Media Gateway Control Protocol
MS:	Mobile Station
MSID:	Mobile Station Identifier
MSISDN:	Mobile Station International Station Directory Number
MT:	Mobile Terminal
MTA:	Multimedia Terminal Adapter
NAI:	Network Access Identifier
NAS:	Network Access Server
OSI:	Open System Interconnection
PBX:	Private Branch Exchange
PC:	Packet Cable
PDP:	Packet Data Protocol
PDSN:	Packet Data Serving Node
PHY:	Physical Access
PINT:	PSTN and Internet Interworking - IETF WG
POP:	Point Of Presence
PPP:	Point to Point Protocol
PSTN:	Public Switched Telephone Network
PVC:	Permanent Virtual Circuit
QoS:	Quality of Service
RADIUS:	Remote Authentication Dial In User Service protocol
RAS:	Registration, Administration, and Status
RSVP:	Resource Reservation Protocol
SCTP:	Stream Control Transmission Protocol
SFID:	Service-Flow-ID
SG:	Signaling Gateway
SID:	System Identification Number
SIP:	Session Initiation Protocol
SNA:	Systems Network Architecture
SONET:	Synchronous Optical Network
SVC:	Switched Virtual Circuit
TIA:	Telecommunication Industry Association
TCP:	Transmission Control Protocol
TDM:	Time Division Multiplexing

TE:	Terminal Equipment
TSP:	Telecommunications Service Provider
UDP:	User Datagram Protocol
VCI:	Virtual Circuit Indicator
VFRAD:	Voice over Frame Relay Access Device
VoFR:	Voice over Frame Relay
VoP:	Voice over Packet
VoIP:	Voice over Internet Protocol
VPI:	Virtual Path Indicator

4 Introduction and Executive Summary

4.1 Convening the JEM

In its Third Report and Order regarding implementation of the Communications Assistance for Law Enforcement Act (CALEA), the FCC finds "that the approach taken [by industry] with regard to packet-mode communications in J-STD-025 raises significant technical and privacy concerns." Under J-STD-025 for packet-mode communications, law enforcement could be provided with access to the full call content stream when only Pen Register or Trap and Trace information was authorized to be delivered.

The FCC "believe[s] that further efforts can be made to find ways to better protect privacy by providing law enforcement only with the information to which it is lawfully entitled." However, the FCC acknowledges that the record before it does not sufficiently address packet technologies and the problems that they may present for CALEA purposes. The FCC notes, for example, "that some packet technologies (e.g., frame relay, ATM, X.25) are connection oriented i.e., there are call set-up and take-down processes, similar to those used in circuit switched voice networks, whereby addressing information is made available to the carrier separate from and before call content is transmitted. Other packet technologies (e.g., Internet protocol based solutions) would not be processed this way."

Accordingly, the FCC invited TIA to study CALEA solutions for packet-mode technology and report in one year on "steps that can be taken, including particular amendments to J-STD-025, that will better address privacy concerns." To meet the deadline imposed by the FCC, and to build a record based on technical facts, the Telecommunications Industry Association (TIA) convened a Joint Experts Meeting.

The JEM was intended to serve as a technical fact-finding body across the spectrum of packet-mode communication technologies regarding the feasibility of delivering less than the full content of a packet to law enforcement in response to a pen register order. Invitations were sent to a broad range of packet-mode communications expert organizations. The invitation list is attached as Appendix B.

To facilitate discussion at the JEM, contributions from various entities were made available through posting on the TIA website prior to meeting in person (see CALEA JEM link at http://www.tiaonline.org/standards/calea_jem). A publicly available mailing list was also maintained. A two-hour question and answer session covering the scope of the JEM was conducted on March 20, 2000.

The first JEM session was conducted on May 3-5, 2000, in Las Vegas, NV. Based on the results of the first JEM, a second JEM session was conducted in Washington D.C., on June 26-29, 2000. The output from those meetings is described below.

4.2 JEM I Output

Following opening remarks, updates were provided on the status of Revision A of J-STD-025, the legal purpose of the JEM, and the status of CALEA activities. Presentations on technical issues followed. A copy of the JEM I meeting agenda is attached as Appendix C.

While the scope of the JEM included reporting on the broadest number of packet-mode communications technologies, contributions were received only on the following technologies: cdma2000, GPRS, and IP. There was broad discussion across many technologies however.

JEM I established a framework for preparing this report. A copy of the JEM I meeting report to TIA TR45 is attached as Appendix D.

First, JEM I concluded that, based on current FCC guidance, it could not define "call-identifying information" for packet services. Several contributors noted that the term "call-identifying information" is ambiguous with regard to packet communications. Instead, JEM I concluded that it could only attempt to identify what information may be available about the packet communication without regard to whether it might be characterized as "call identifying information" under CALEA. . Once the information was identified, JEM I concluded that it could then report on the technical impact and feasibility of making that information available to a law enforcement agency (LEA). This decision was consistent with the purpose and scope of the JEM, which did not include discussion of legal issues.

Second, JEM I noted that CALEA requirements apply to telecommunication services not information services. JEM I recognized, however, that from a packet point of view, the two may be indistinguishable. JEM I determined that it is not technically advisable to determine, on a packet by packet basis, the application or communication services that is being provided. JEM I also concluded that, the application or communication services that is being provided can not be determined even by observation of the complete stream of packets. The point of communications setup may be the only time that a telecommunication service can be distinguished from an information service.

JEM I further concluded that the possibility of encapsulation or encryption of packets outside of the service provider's control makes identifying the application or service even more unlikely.

JEM I addressed the issues related to packet-mode services in two main categories: (1) packet communication sessions established by a Call Management Server (CMS), and (2) transport services, (i.e. packet communication sessions established without a CMS). The CMS may, for instance, be an H.323 GateKeeper, or a SIP proxy, or something conceptually equivalent. Typically, an access service provider that offers a CMS also provides transport.

Accordingly, the framework for this report reflects this two-pronged approach. In each category, JEM I decided to report on the information available and the technical impact of providing it. Because further information was necessary, a second JEM meeting was scheduled to accept contributions for technologies and assignments were taken to prepare appendices of technologies for this report.

Finally, JEM I agreed that if a change to the current standard (J-STD-025) were deemed necessary by the Federal Communications Commission, a court or the industry, as a result of this process, the JEM recommends that the open, joint ATIS T1/TIA activity currently underway in TIA TR45.2 LAES Ad Hoc be responsible for completing this task. In its simplest form, this change may just be the inclusion of appropriate references to other standards. Nothing in this process, however, was intended to or should preclude any standards setting or industry organization from adopting their own "safe harbor" standard for their particular technology (e.g., satellite or cable standards).

4.3 JEM II Output

Contributions to JEM II were received in advance of the meeting and made available on the TIA website. Technologies covered in the contributions included: cdma2000 Wireless IP, X.25 over ISDN, ATM, Frame Relay, GPRS, PacketCable, CDPD, and IP.

Following opening remarks, updates were provided on the status of Revision A of J-STD-025 as well as the pending appeal before the U.S. Court of Appeals for the District of Columbia of the FCC Report and Order. Presentations on technical issues followed.

A copy of the JEM II meeting agenda is attached as Appendix E and a copy of the JEM II meeting report to TIA TR45 is attached as Appendix F.

In addition to the contributions based on assignments from JEM I, the CALEA Implementation Section (CIS) of the Federal Bureau of Investigation (FBI) submitted a contribution that proposed a functional approach to separating packet content from packet identifying information. Further, the FBI requested the opportunity to present technology it currently uses to separate identifying information from content known as "Carnivore."

The Carnivore presentation was provided by law enforcement's Data Intercept Technology Program at the FBI's Engineering Research Facility from Quantico, Virginia. The presenters described the current law enforcement techniques for separating identifying information from content to comply with lawfully authorized surveillance orders. In summary, law enforcement, in cooperation with a service provider pursuant to legal authorization, gains access to a packet stream in which the target's communications reside. The access is made on the service provider's premises using law enforcement equipment.

According to the presenters, the target's communications are identified through use of a filtering program developed by law enforcement. In a Pen Register or Trap and Trace Order only the relevant information from the target's packets are stored to disk. The filter

program separates the relevant information from the target's content and law enforcement then collects the information.

The presenters informed JEM II that development of the filter protocol was intensive and fluid because of the ever changing nature of packet protocols and the constant introduction of new protocols; the Carnivore software or filters may need to be updated almost weekly to stay current. Carnivore has not been proven effective, as yet, in cases where the subject's communications are part of a high bandwidth transmission. The presenters acknowledged that to require service providers to develop and maintain similar Carnivore-like software would be extremely burdensome.

CIS then presented its contribution, which suggested "examining the full packet stream from the subject in order to gather the relevant call-identifying information for delivery to the LEA." CIS acknowledged in its contribution, however, that "examine[ing] the full packet stream and examine protocol layers higher than layer 3 would place a high load on existing network elements in most architectures." Accordingly, using the J-STD-025 functional approach to surveillance, CIS suggested that "the access function unobtrusively captures the complete subject packet stream (including all call content and call-identifying information) and distributes it to the delivery function." The delivery function in the contribution contains a new "sub function" referred to as a Separation Function. The Separation Function would remove "any information the LEA may not be entitled to based on the court order [so that in] the case of Title I court orders, all communication content information would be removed." The delivery function would then deliver the identifying information to the LEA's collection function.

CIS did not recommend any specific implementation or ownership of the Separation Function. CIS acknowledged that "development of separation capabilities (i.e. filtering capabilities) within a service provider's network may be unrealistic as it would be highly resource intensive, very inefficient, and potentially inconsistent between providers". For these and other reasons described below there was industry consensus in subsequent discussions that it would not be feasible developing such a Separation Function independently or through a standards based process. To address these issues while also addressing privacy concerns, it was discussed that Carnivore-like software could be made available to service providers so that the Separation Function occurred under service provider management.

JEM II agreed that Carnivore, as presented by CIS, constitutes a potential technical solution for separating content from packet information and therefore is included within the JEM report. However, numerous industry concerns were raised about the introduction of government-provided product into the service provider network. Concerns were acknowledged regarding (a) potential liability for failure of the product, (b) uncertain impact on the network, (c) terms and conditions to obtain the product from government, (d) administrative and operational impacts from constant upgrades to the filter, (e) scalability, (f) privacy, (g) certification or testing of the product, and (h) uncertainty about the scope of the filter (i.e., whether the filter produces information

that is coextensive with call identifying information and who establishes the criteria for separation).

A Compaq contribution recommended that a similar filtering technology be developed by an independent, third party entity as open source code. This solution attempts to (1) overcome potential privacy concerns with a solely law enforcement-developed filter, and (2) take advantage of the opportunity provided by an open source model to receive rapid input on new packet protocols as they are developed. As with the FBI-proposed filter, there are many industry concerns regarding the implementation of an open source solution.

Nonetheless, JEM II recognized CIS and Compaq contributions as valuable additions to the process. There was consensus that the technological solution would be included in the report but that the legal, policy and implementation issues would not be addressed and were beyond the scope of the report. For example, JEM II does not address the potential impact of a Carnivore solution being implemented within the delivery function. The potential solution would require additional study. It was also noted that the current packet-mode solution in J-STD-025 is less intrusive from a privacy perspective than law enforcement's current Carnivore implementation because under the existing standard only the packet stream known by the service provider to be associated with the subject will be delivered to the LEA collection function in contrast to law enforcement's current practice of attaching Carnivore to a packet stream that will contain packets from a number of different users.

JEM II expressed its appreciation to CIS for arranging the Carnivore presentation and for its technical contribution to the JEM, which was incorporated into the report.

In addition to the CIS contribution, contributions regarding other technologies were reviewed, accepted, and incorporated as appendices to the report. It was agreed that the report would be posted on the TIA website for further review and comment before completion of the JEM process and forwarding to TIA.

5 Packet Communication Sessions established by a Call Management Server

This section describes the environment in which call based services are provided using a Call Management Server (CMS). A CMS facilitates the establishment of end-to-end protocols such as H.323 or SIP. The following material in this section assumes that the CMS is capable of providing call events. If the CMS does not provide call events then the discussion in section 6 applies.

5.1 Information that can be reported

Information available is analogous to J-STD-025 call events, but with respect to each technology, enhancements may need to be made to J-STD-025. For example, with respect to Voice-over-Packet (VoP) services, the JEM notes that additional enhancements are needed to J-STD-025 (e.g., to report VoP calls and associated Pen Register or Trap and Trace information, to identify the content stream, and to identify the timing requirements). Other standards may address other technologies and networks.

5.2 Technical Impacts

The provider will indicate to law enforcement the negotiated service (e.g. user's session negotiation), however, the user may use the service differently than negotiated. For example, in a voice over packet call the user may be using the service to send or receive other than voice information. Thus, law enforcement may be expecting information regarding a voice call but receive some other content.

Interception of packet services also does not guarantee that the packets have been received by the terminating system.

H.323 and SIP call events may not map directly to those call events established in J-STD-025 (e.g., triggering events may be different). Impacts associated with development of a protocol to support reporting packet data communication call events have not yet been investigated and there may be unforeseen issues.

Timing requirements need to be reviewed and may need to be specified for each technology.

The JEM did not address possible difficulties in associating call events with call content as required by CALEA.

6 Packet Communication Sessions established without a Call Management Server

This section describes the environment for service providers that provide packet-mode transport, without the involvement of a CMS.

6.1 Information that can be reported, subject to technical impact analysis

Establishment of a communication path across an accessing system from the subject's device to a network (not the endpoint) may be required before communication between the subject and associate can begin. If so, the establishment and release of this path could be reported. The information provided may be technology-dependent.

Reporting of information beyond establishment and release requires access to the individual packets, which may yield further information such as non-encapsulated routing information. Alternatively, the entire packet could be delivered. It must be noted that either may be difficult and not feasible for some existing systems and architectures, as discussed below.

6.2 Technical Impacts

For all of the delivery options discussed below, the following comments apply:

- the consensus is that in many technologies the duplication of a packet stream requires significant resources. These resources compete with the Title III resources as well as capacity requirements;
- the subscriber under surveillance, and their associates, may detect performance degradation resulting from the impact of duplication of a packet stream for every Pen Register or Trap and Trace. Other customers using the packet data services of the TSP may also detect the degradation of performance. The JEM notes that a single subscriber to the packet transport service may utilize excessive packet capacity;
- It is assumed that the subscriber under surveillance can be readily identified within the network by the technology specific identifiers listed in the appendices.

6.2.1 Delivering the Entire Packet Stream

Currently J-STD-025 specifies delivery of the entire packet stream or just the Source and Destination address information for a user under surveillance. While delivery of the entire packet stream guarantees that authorized Pen Register and Trap and Trace information will be delivered to the LEA, it does not remove content prior to delivery. This places the responsibility on the LEA to retain only the authorized information, which has been raised as a potential issue by the privacy groups. The JEM noted that under this method, only the packets for the user under surveillance are delivered, and not

those for other users on the system. Since the LEA has no access to the packets from other users on the system, this does represent an improvement from the current state of the art.¹

6.2.2 Delivery of Header routing information

The JEM agreed that a TSP could extract the packet header routing information from the packet content associated with a user under surveillance. It was noted that only providing this information (i.e. the source and destination address information) might not give LEAs access to all the necessary Pen Register or Trap and Trace information. Specifically, the IP addressing information that could be provided by an IP service provider may not meaningfully identify either the subject or associate due to IP capabilities such as Network Address Translation and dynamic IP addressing. For example, information contained in the IP data field, such as email addresses, would not be provided with the routing information.

6.2.3 Extraction of Pen Register or Trap and Trace information

Relevant Pen Register or Trap and Trace information may be located in different layers of the protocol depending on the specific service used and the application of the packet (e.g., a POP e-mail packet vs. a connection setup packet for H.323 or SIP service). The variability of applications therefore makes it difficult for a service provider to extract such information. New services (and therefore application layer protocols) are developed on a continual basis within the IP environment making isolation of Pen Register or Trap and Trace information within an IP data field even more complicated. If a separation capability were to be developed, maintaining accurate and up-to-date separation capabilities (i.e., filtering capabilities) will require rapid, continuous development which will be highly resource intensive. This process does not lend itself to the current standards development process due to the process' sometimes lengthy, consensus driven nature. It is also expected that the industry resources for this work would be significantly greater than the resources that are currently committed for surveillance standards development.

The JEM did not have sufficient information to determine whether or not an extraction solution would be scalable in the quantity deployments anticipated under CALEA, especially as the filtering becomes more complex and the network speeds increase. Additionally, there may be significant administrative and operational challenges to keeping the extraction function useful and accurate once all of the complications outlined in the IP Appendix (e.g. encapsulation, fragmentation, independent packet routing, and encryption) are taken into consideration. Further, because implementation issues were beyond the scope of the JEM, technical issues with respect to functional implementation such as capacity needs and impact on other Network elements (i.e., whether the extraction function is located within the service provider network) were not identified.

¹ The packet processing equipment used in most present day Telecommunication Service Provider networks does not include a capability to extract the packet stream for a particular user.

The above considerations are magnified as access speeds increase to gigabit/sec and faster. High-speed technologies may not permit time to investigate the packet.

Delivery of the FCC mandated timing requirement of eight seconds needs to be reviewed and may need to be specified for each technology and each solution discussed above.